Frank S. Hedin (SBN 291289)
Hedin LLP
535 Mission Street, 14th Floor
San Francisco, CA 94105
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
E-Mail: fhedin@hedinllp.com

Counsel for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

TERESA TURNER, individually and on behalf of all others similarly situated, Plaintiff, V. NATIONAL NOTARY ASSOCIATION, Defendant.	Case No. 2:25-cv-334 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Teresa Turner, individually and on behalf of all others similarly situated, makes the following allegations pursuant to the investigation of counsel and based upon information and belief, except as to allegations pertaining specifically to herself or her counsel, which are based on personal knowledge.

A. NATURE OF THE CASE

1. Plaintiff brings this action to redress Defendant's practice of selling, renting, transmitting, and/or otherwise disclosing to Meta, records containing the

personal information of each of its customers, along with detailed information revealing the titles and subject matter of the videos and other audiovisual materials purchased by each customer in violation of the Video Privacy Protection Act, 18 U.S.C. § 2710 et seq. ("VPPA").

2. Over the past two years, Defendant has systematically transmitted (and continue to transmit today) its customers' personally identifying video viewing information to third parties, such as Meta Platforms, Inc. ("Meta"). The programming code for Meta is called the "Meta Pixel," which Defendant chose to install on the www.nationalnotary.org website.

3. The information Defendant disclosed (and continues to disclose) to Meta via the Meta Pixel includes the customer's Facebook ID ("FID") and the specific title of prerecorded videos that each of its customers purchased on Defendant's Website. An FID is a unique sequence of numbers linked to a specific Meta profile. A Meta profile, in turn, identifies by name the specific person to whom the profile belongs (and also contains other personally identifying information about the person). Entering "Facebook.com/[FID]" into a web browser returns the Meta profile of the person to whom the FID corresponds. Thus, the FID identifies a person more precisely than a name, as numerous persons may share the same name, but each person's Facebook profile (and associated FID) uniquely identifies one and only one person. In the simplest terms, the Meta Pixel installed by Defendant captures and discloses to Meta

information that reveals a particular person purchased a specific title of a prerecorded video on Defendant's Website (hereinafter, "Private Video Information").

4. Defendant disclosed and continue to disclose its customers' Private Video Information to Meta without asking for, let alone obtaining, their consent to these practices.

5. The VPPA clearly prohibits what Defendant has done. Subsection (b)(1) of the VPPA provides that, absent the consumer's prior informed, written consent, any "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for," 18 U.S.C. § 2710(b)(1), damages in the amount of $2,500.00, *see id.* § 2710(c).

6. Accordingly, on behalf of herself and the putative Class members defined below, Plaintiff brings this Class Action Complaint against Defendant for intentionally and unlawfully disclosing her and Putative Class members' Private Video Information to Meta.

B. PARTIES

I. Plaintiff Teresa Turner

7. Plaintiff is, and at all times relevant hereto was, a citizen and resident of San Luis Obispo County, California.

8. Plaintiff is, and at all times relevant hereto was, a user of Meta.

9. Plaintiff is a consumer of the video products and services offered on Defendant's www.nationalnotary.org website. Including on or about August 2024, Plaintiff purchased prerecorded video material from Defendant's www.nationalnotary.org website by requesting and paying for such material, providing her name, email address, and home address for delivery of such material. Defendant completed the sales of goods to Plaintiff by shipping or delivering the prerecorded video material she purchased to the address she provided in her order. Accordingly, Plaintiff requested or obtained, and is therefore a consumer of, prerecorded video material sold by Defendant on its website.

10. At all times relevant hereto, including when requesting or obtaining prerecorded video material from Defendant's website, Plaintiff had a Meta account, a Meta profile displaying her name and picture, and an FID associated with such profile.

11. Plaintiff has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Private Video Information to Meta. In fact, Defendant has never even provided Plaintiff with written notice of its practices of disclosing its customers' Private Video Information to third parties such as Meta.

12. Prior to and at the time she purchased prerecorded video material from Defendant, Defendant did not notify Plaintiff that it would disclose the Private Video Information of its customers generally or that of Plaintiff in particular, and Plaintiff has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her

Private Video Information to third parties. Plaintiff has never been provided any written notice that Defendant discloses its customers' Private Video Information or any means of opting out of such disclosures of her Private Video Information.

13. Because Defendant disclosed Plaintiff's Private Video Information (including her FID, unique identifiers, and her request or purchase of prerecorded video material from Defendant's website) to third parties during the applicable statutory period, Defendant violated Plaintiff's rights under the VPPA and invaded her statutorily conferred interest in keeping such information (which bears on her personal affairs and concerns) private.

II. Defendant

14. Defendant National Notary Association is a not-for-profit corporation organized under the laws of California, with its headquarters at 9350 De Soto Ave., Chatsworth, California 91311. Defendant is the largest and oldest organization in the United States serving notaries and training persons to be notaries through certifications, trainings, seminars, conferences, and printed and online educational materials that accompany these programs.

C. JURISDICTION AND VENUE

15. The Court has subject-matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.

16. Personal jurisdiction and venue are proper because Defendant maintains its headquarters and principal place of business in Los Angeles, California, within this judicial District.

VIDEO PRIVACY PROTECTION ACT

17. The VPPA prohibits companies (like Defendant) from knowingly disclosing to third parties (like Meta) information that personally identifies consumers (like Plaintiff) as having requested or obtained specific video(s) or other audio-visual materials from its Website.

18. Specifically, subject to certain exceptions that do not apply here, the VPPA prohibits "a video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider[.]" 18 U.S.C. § 2710(b)(1). The statute defines a "video tape service provider" as "any person, engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials," 18 U.S.C. § 2710(a)(4). It defines a "consumer" as "a renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). "'[P]ersonally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).

19. Leading up to the VPPA's enactment in 1988, members of the United States Senate warned that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." *Id.* Senators at the time were particularly troubled by disclosures of records that reveal consumers' purchases and rentals of videos and other audiovisual materials because such records offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy, respectively).

20. Thus, in proposing the Video and Library Privacy Protection Act (which later became the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont from 1975 to 2023) sought to codify, as a matter of law, that "our right to privacy protects the choice of movies that we watch with our family in our own homes." 134 Cong. Rec. S5399 (May 10, 1988). As Senator Leahy explained at the time, the personal nature of such information, and the need to protect it from disclosure, is the raison d'être of the statute: "These activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people." *Id.*

21. While these statements rang true in 1988 when the act was passed, the importance of legislation like the VPPA in the modern era of data mining is more pronounced than ever before. During a more recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy emphasized the point by stating: "While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[1]

22. Former Senator Al Franken may have said it best: "If someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure that consumers have the right to easily control who finds out what they watch—and who doesn't. The Video Privacy Protection Act guarantees them that right."[2]

23. In this case, however, Defendant deprived Plaintiff and numerous other similarly situated persons of that right by systematically (and surreptitiously)

---

[1] The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, http://www.judiciary. senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the- 21stcentury.

[2] Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century, franken.senate.gov (Jan. 31, 2012).

disclosing their Private Video Information to Meta, without providing notice to (let alone obtaining consent from) any of them, as explained in detail below.

BACKGROUND FACTS

I. Consumers' Personal Information Has Real Market Value

24. In 2001, Federal Trade Commission ("FTC") Commissioner Orson Swindle remarked that "the digital revolution . . . has given an enormous capacity to the acts of collecting and transmitting and flowing of information, unlike anything we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves."[3]

25. Over two decades later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a 26 billion dollar per year online advertising industry in the United States.[4]

26. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

[3] Transcript, *The Information Marketplace* (Mar. 13, 2001), at 8-11, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[4] *See* Julia Angwin and Emily Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), available at https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[5]

27. In fact, an entire industry exists while companies known as data aggregators purchase, trade, and collect massive databases of information about consumers. Data aggregators then profit by selling this "extraordinarily intrusive" information in an open and largely unregulated market.[6]

28. The scope of data aggregators' knowledge about consumers is immense: "If you are an American adult, the odds are that [they] know[] things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on."[7]

---

[5] Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, available at https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf

[6] *See* M. White, *Big Data Knows What You're Doing Right Now*, TIME.com (July 31, 2012), available at http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/ .

[7] N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012), available at https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html#:~:text=It's%20called%20the%20Acxiom%20Corporation,to%20know%20much%2C%20much%20more.

29. Further, "[a]s use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of information about consumers that are now available."[8]

30. Recognizing the severe threat the data mining industry poses to consumers' privacy, on July 25, 2012, the co-chairmen of the Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking information on how those companies collect, store, and sell their massive collections of consumer data, stating in pertinent part:

> By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on every U.S. consumer. This large[-]scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns.[9]

31. Data aggregation is especially troublesome when consumer information is sold to direct-mail advertisers. In addition to causing waste and inconvenience, direct-mail advertisers often use consumer information to lure unsuspecting consumers

---

[8] Letter from Sen. J. Rockefeller IV, Sen. Cmtee. On Commerce, Science, and Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) available at https://www.commerce.senate.gov/services/files/3bb94703-5ac8-4157-a97b-%20a658c3c3061c.

[9] *See Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers' Personal Information*, Website of Sen. Markey (July 24, 2012), available at https://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information.

into various scams, including fraudulent sweepstakes, charities, and buying clubs. Thus, when companies like Defendant share information with data aggregators, data cooperatives, and direct-mail advertisers, they contribute to the "[v]ast databases" of consumer data that are often "sold to thieves by large publicly traded companies," which "put[s] almost anyone within the reach of fraudulent telemarketers" and other criminals.[10]

32. Disclosures like Defendant's are particularly dangerous to the elderly. "Older Americans are perfect telemarketing customers, analysts say, because they are often at home, rely on delivery services, and are lonely for the companionship that telephone callers provide."[11]

33. The FTC notes that "[t]he elderly often are the deliberate targets of fraudulent telemarketers who take advantage of the fact that many older people have cash reserves or other assets to spend on seemingly attractive offers."[12]

34. Indeed, an entire black market exists while the personal information of vulnerable elderly Americans is exchanged. Thus, information disclosures like

[10] *See* Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. Times (May 20, 2007), available at https://www.nytimes.com/2007/05/20/business/20tele.html.

[11] *Id*.

[12] Prepared Statement of the FTC on "Fraud Against Seniors" before the Special Committee on Aging, United States Senate (August 10, 2000).

Defendant's are particularly troublesome because of their cascading nature: "Once marked as receptive to [a specific] type of spam, a consumer is often bombarded with similar fraudulent offers from a host of scam artists."[13]

35. Defendant is not alone in violating its customers' statutory rights and jeopardizing their well-being in exchange for increased revenue: disclosing customer and subscriber information to data aggregators, data appenders, data cooperatives, direct marketers, and other third parties has become a widespread practice. Unfortunately for consumers, however, this growth has come at the expense of their most basic privacy rights.

II. Consumers Place Monetary Value on Their Privacy and Consider Privacy Practices When Making Purchases

36. As the data aggregation industry has grown, so has consumer concerns regarding personal information.

37. A survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies who they believe do protect their privacy online.[14] As a result, 81 percent of smartphone

[13] *Id*.

[14] *See 2014 TRUSTe US Consumer Confidence Privacy Report*, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.[15]

38. Thus, as consumer privacy concerns grow, consumers increasingly incorporate privacy concerns and values into their purchasing decisions, and companies viewed as having weaker privacy protections are forced to offer greater value elsewhere (through better quality and/or lower prices) than their privacy-protective competitors. In fact, consumers' personal information has become such a valuable commodity that companies are beginning to offer individuals the opportunity to sell their personal information themselves.[16]

39. These companies' business models capitalize on a fundamental tenet underlying the personal information marketplace: consumers recognize the economic value of their private data. Research shows that consumers are willing to pay a premium to purchase services from companies that adhere to more stringent policies of protecting their personal data.[17]

---

[15] *Id*.

[16] *See* Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012), available at https://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html.

[17] *See* Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (2011); *see also* European Network and Information Security Agency, *Study on Monetizing Privacy*

40. Thus, in today's digital economy, individuals and businesses alike place a real, quantifiable value on consumer data and corresponding privacy rights.[18] As such, where a business offers customers a product or service that includes statutorily guaranteed privacy protections, yet fails to honor these guarantees, the customer receives a product or service of less value than the product or service paid for.

III. Defendant Use the Meta Pixel to Systematically Disclose its customers' Private Video Information to Meta

41. As alleged below, when a consumer requests or obtains a particular prerecorded video on Defendant's Website, the Meta Pixel technology that Defendant intentionally installed on its Website transmits (1) the unencrypted FID for each purchaser; (2) detailed information revealing the titles and subject matter of the prerecorded videos requested or obtained by each of its purchasers; and (3) the URL where such videos are available for purchase, without the consumer's consent and in clear violation of the VPPA.

(Feb. 27, 2012), available at https://www.enisa.europa.eu/publications/monetising-privacy.

[18] *See* Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, available at https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf.

A. The Meta Pixel

42. On February 4, 2004, Mark Zuckerberg and others launched Facebook, now known as "Meta".[19] Meta is now the world's largest social media platform. To create a Meta account, a person must provide, *inter alia*, his or her first and last name, birth date, gender, and phone number or email address.

43. The Meta Pixel, first introduced in 2013 as the "Facebook Pixel," is a unique string of code that companies can embed on their websites to monitor and track the actions taken by visitors to their websites and to report them back to Meta. This allows companies like Defendant to build detailed profiles about its customers and to serve them with highly targeted advertising.

44. Additionally, the Meta Pixel installed on a company's website allows Meta to "match [] website visitors to their respective Facebook User accounts."[20] This is because Meta has assigned to each of its users an "FID" number – a unique and persistent identifier that allows anyone to look up the user's unique Meta profile and thus identify the user by name[21] – and because each transmission of information made

[19] *See* Facebook, "Company Info," available at https://about.fb.com/company-info./.

[20] Meta, "Get Started – Meta Pixel," available at https://developers.facebook.com/docs/meta-pixel/get-started/.

[21] For example, Mark Zuckerberg's FID is reportedly the number "4," so logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark

from a company's website to Meta via the Meta Pixel is accompanied by, *inter alia*, the FID of the website's visitor.

45. As Meta's developer's guide explains, installing the Meta Pixel on a website allows Meta to track actions that users with Meta accounts take on the site. Meta states that "Examples of [these] actions include adding an item to their shopping cart or making a purchase."[22]

46. Meta's Business Tools Terms govern the use of Meta's Business Tools, including the Meta Pixel.[23]

47. Meta's Business Tools Terms state that website operators may use Meta's Business Tools, including the Meta Pixel, to transmit the "Contact Information" and "Event Data" of their website's visitors to Meta.

48. Meta's Business Tools Terms define "Contact Information" as "information that personally identifies individuals, such as names, email addresses, and phone numbers . . . ."[24]

Zuckerberg's Facebook page: www.facebook.com/zuck, and all of the additional personally identifiable information contained therein.

[22] Meta, "About Meta Pixel," available at https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[23] Meta, "Meta Business Tools Terms," available at https://www.facebook.com/legal/technology_terms.

[24] *Id*.

49. Meta's Business Tools Terms state: "You instruct us to process the Contact Information solely to match the Contact Information against user IDs [e.g., FIDs] ("Matched User IDs"), as well as to combine those user IDs with corresponding Event Data."[25]

50. The Business Tools Terms define "Event Data" as, *inter alia*, "information that you share about people and the actions that they take on your websites and apps or in your shops, such as visits to your sites, installations of your apps, and purchases of your products."[26]

51. Website operators use the Meta Pixel to send information about visitors to their Websites to Meta. Every transmission to Meta accomplished through the Meta Pixel includes at least two elements: (1) the website visitor's FID and (2) the webpage's URL triggering the transmission.

52. Depending on the configuration of the Meta Pixel, the website may also send Event Data to Meta. Defendant have configured the Meta Pixel on its Website to send Event Data to Meta.

[25] *Id.*

[26] *Id.*

53. When website operators make transmissions to Meta through the Meta Pixel, none of the following categories of information are hashed or encrypted: the visitor's FID, the website URL, or the Event Data.

54. Every website operator installing the Meta Pixel must agree to the Meta Business Tools Terms.[27]

55. Moreover, the Meta Pixel can follow a consumer to different websites and across the Internet even after the consumer's browser history has been cleared.

56. Meta has used the Meta Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its billions of users worldwide, including information about all of its users' interactions with any of the millions of websites across the Internet on which the Meta Pixel is installed. Meta then monetizes this Orwellian database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

57. Simply put, if a company chooses to install the Meta Pixel on its website, both the company who installed it and Meta (the recipient of the information it

[27] *See id.*

transmits) are then able to "track [] the people and type of actions they take,"[28] including, as relevant here, the specific prerecorded video material that they purchase from Defendant's website.

B. Defendant Knowingly Uses the Meta Pixel to Transmit the Private Video Information of its Customers to Meta

58. Defendant sells various prerecorded video materials on its Website, www.nationalnotary.org, including online courses and certification programs on various topics, including becoming a licensed notary or signing agent.

59. To purchase prerecorded video material from both Defendant's Website, a person must provide at least his or her name, email address, billing address, and credit or debit card (or other form of payment) information.

60. During the purchase process on Defendant's Website, Defendant uses – and has used at all times relevant hereto – the Meta Pixel to disclose to Meta the unencrypted FID of the person who made the purchase and the specific title of video material that the person purchased (as well as the URL where such video material is available for purchase).

[28] Meta, "Retargeting: How to Advertise to Existing Customers with Ads on Facebook," available at https://www.facebook.com/business/goals/retargeting?checkpoint_src=any.

61. In order to take advantage of the targeted advertising and other informational and analytical services offered by Meta, Defendant intentionally programmed its Website (by following step-by-step instructions from Meta's website) to include the Meta Pixel code, which systematically transmits to Meta the FID of each person with a Meta account who purchases prerecorded video material on Defendant's Website, along with the specific title of the prerecorded video material that the person purchased.

62. With only a person's FID and the title of the prerecorded video material (or URL where such material is available for purchase) that the person purchased from Defendant's Website —all of which Defendant knowingly and systematically provides to Meta—any ordinary person could learn the identity of the person to whom the FID corresponds and the subscription or the title of the specific prerecorded video material that the person purchased (and thus requested and obtained). This can be accomplished simply by accessing the URL www.facebook.com/ and inserting the person's FID.

63. Defendant's practice of disclosing the Private Video Information of its customers to Meta continued unabated for the duration of the two-year period preceding the filing of this action. At all times relevant hereto, whenever Plaintiff or any other person purchased prerecorded video material from Defendant on its Website, Defendant disclosed to Meta (*inter alia*) the specific title of the video material that was requested or obtained (including the URL where such material is available for

purchase), along with the FID of the person who requested or obtained it (which, as discussed above, uniquely identified the person).

64. At all times relevant hereto, Defendant knew the Meta Pixel was disclosing its customers' Private Video Information to Meta.

65. Although Defendant could easily have programmed its Website so that none of its customers' Private Video Information is disclosed to Meta, Defendant instead chose to program its Website so that all of its customers' Private Video Information is disclosed to Meta.

66. Before transmitting its customers' Private Video Information to Meta, Defendant failed to notify any of them that it would do so, and none of them have ever consented (in writing or otherwise) to these practices.

67. By intentionally disclosing to Meta Plaintiff's and their other customers' FIDs together with the specific title of the prerecorded video material that they each purchased, without any of their consent to these practices, Defendant knowingly violated the VPPA on an enormous scale.

CLASS ACTION ALLEGATIONS

68. Plaintiff seeks to represent a class defined as all persons in the United States who, during the two years preceding the filing of this action, purchased prerecorded video material or services from Defendant's Website while maintaining an account with Meta Platforms, Inc. f/k/a Facebook, Inc.

69. Class members are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in at least the tens of thousands. The precise number of Class members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the Defendant's membership records.

70. Common questions of law and fact exist for all Class members and predominate over questions affecting only individual class members. Common legal and factual questions include but are not limited to (a) whether Defendant embedded Meta Pixel on its Website that monitors and tracks actions taken by visitors to its Website; (b) whether Defendant reports the actions and information of visitors to Meta; (c) whether Defendant knowingly disclosed Plaintiff's and Class members' Private Video Information to Meta; (d) whether Defendant's conduct violates the Video Privacy Protection Act, 18 U.S.C. § 2710; and (e) whether Plaintiff and Class members are entitled to a statutory damage award of $2,500, as provided by the VPPA.

71. The named Plaintiff's claims are typical of the claims of the Class in that the Defendant's conduct toward the putative class is the same. That is, Defendant embedded the Meta Pixel on its Website to monitor and track actions taken by consumers on its Website and report this to Meta. Further, the named Plaintiff and the Class members suffered invasions of their statutorily protected right to privacy (as

afforded by the VPPA), as well as intrusions upon their private affairs and concerns that would be highly offensive to a reasonable person, as a result of Defendant's uniform and wrongful conduct in intentionally disclosing their Private Purchase Information to Meta.

72. Plaintiff is an adequate representative of the Class because she is interested in the litigation; her interests do not conflict with those of the Class members she seeks to represent; she has retained competent counsel experienced in prosecuting class actions; and she intends to prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the interests of all Class members.

73. The class mechanism is superior to other available means for the fair and efficient adjudication of Class members' claims. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by this case's complex legal and factual issues. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication of the common questions of law and fact, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability

issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSE OF ACTION
Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710

74. Plaintiff repeats the allegations asserted in the preceding paragraphs as if fully set forth herein.

75. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

76. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]" Defendant are each a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because they engaged in the business of selling and delivering prerecorded video materials, similar to prerecorded video cassette tapes, to consumers nationwide.

77. As defined in 18 U.S.C. § 2710(a)(1), a "'consumer' means any renter, purchaser, or consumer of goods or services from a video tape service provider." As alleged above, Plaintiff and Class members are each a "consumer" within the meaning

of the VPPA because they each purchased prerecorded video material or services from Defendant's Website that were sold and delivered to them by Defendant.

78. As defined in 18 U.S.C. § 2710(a)(3), "'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." The Private Video Information that Defendant transmitted to Meta constitutes "personally identifiable information" as defined in 18 U.S.C. § 2710(a)(3) because it identified Plaintiff and Class members to Meta as an individual who "requested or obtained," specific prerecorded video material from Defendant's Website.

79. Defendant knowingly disclosed Plaintiff's and Class members' Private Video Information to Meta via the Meta Pixel technology because Defendant intentionally installed and programmed the Meta Pixel code on its Website, knowing that such code would transmit the prerecorded video material requested or obtained by their consumers and the consumers' unique identifiers (including FIDs).

80. Defendant failed to obtain informed written consent from Plaintiff or Class members authorizing Defendant to disclose their Private Video Information to Meta or any other third party. More specifically, at no time prior to or during the applicable statutory period did Defendant obtain from any person who requested or obtained prerecorded video material or services on Defendant's Website (including Plaintiff or Class members) informed, written consent that was given in a form distinct

and separate from any form setting forth other legal or financial obligations of the consumer, that was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner, or that was given after Defendant provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

81. By disclosing Plaintiff's and Class members' Private Video Information, Defendant violated their statutorily protected right to privacy in their Private Video Information.

82. Consequently, Defendant is liable to Plaintiff and Class members for damages in the statutorily set sum of $2,500. 18 U.S.C. § 2710(c)(2)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks a judgment against Defendant as follows:

a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as the representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b) For an order declaring that Defendant's conduct as described herein violated the VPPA;

c) For an order finding in favor of Plaintiff and the Class and against Defendant on all counts asserted herein;

d) For an award of $2,500.00 to Plaintiff and each Class member, as provided by 18 U.S.C. § 2710(c);

e) For an order permanently enjoining Defendant from disclosing the Private Video Information of its subscribers to third parties in violation of the VPPA;

f) For prejudgment interest on all amounts awarded; and

g) For an order awarding punitive damages, reasonable attorneys' fees, and costs to counsel for Plaintiff and the Class under Rule 23 and 18 U.S.C. § 2710(c).

Dated: January 13, 2025

Respectfully submitted,

HEDIN LLP

By: /s/ *Frank S. Hedin*

FRANK S. HEDIN (SBN 291289)
535 Mission Street, 14th Floor
San Francisco, CA 94105
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
E-Mail: fhedin@hedinllp.com

Counsel for Plaintiff and the Putative Class